ABSTRACT

A method, and a corresponding apparatus, provide for remote, secure replacement of private keys in a private key infrastructure. The method is implemented as a secure key replacement protocol (SKRP), which includes the steps of receiving a rekey request, where the rekey request identifies a private key for replacement, authenticating the rekey request, replacing the identified private key with a SKRP key, signing the challenge with the SKRP key, and returning the signed challenge. The rekey request includes the SKRP key and the challenge.